Functionaris voor Gegevensbescherming
Postadres Postbus 16200, 3500 CE Utrecht
Telefoon 14 030
www.utrecht.nl
FG@utrecht.nl

Gemeente Utrecht

Verslag Functionaris voor Gegevensbescherming Januari 2025 - Juni 2025

Aan **Gemeenteraad** **College van Burgemeester en Wethouders**		**Datum** 7-10-2025
Van **Functionaris voor Gegevensbescherming**	**Versienummer** 1.1	**Status** Definitief
Kopie Concerndirectie CIO Office	**Bijlagen** 1. Voorbeelden generieke ICT-voorzieningen 2. Voorbeelden standaarden 3. FG jaarverslag 2022-2023	

Inhoudsopgave

Managementsamenvatting

Doel en karakter van het verslag

Dit verslag bevat de eerste waarnemingen van de nieuwe Functionaris voor Gegevensbescherming (FG) over de stand van gegevensbescherming binnen de gemeente Utrecht. De FG benoemt zowel positieve ontwikkelingen als structurele aandachtspunten, en doet aanbevelingen voor verdere versterking van beleid, uitvoering en toezicht. Het verslag bouwt deels voort op het integrale verslag over 2022-2023 van de vorige FG. Over 2024 bracht de vorige FG geen verslag meer uit. Waarnemingen zijn gebaseerd op advisering ten aanzien van tientallen uitgevoerde DPIA's en andere adviesgesprekken gevoerd met organisatieonderdelen – waaronder naar aanleiding van incidenten - in de periode januari tot en met juni 2025. Voor de totstandkoming van dit verslag zijn geen specifieke aanvullende onderzoeken uitgevoerd.

Strategische sturing en ontwikkelrichting

De gemeente heeft de afgelopen jaren geïnvesteerd in een stevig beleidsfundament en een functionele gegevensbeschermingsorganisatie. Dit biedt een goede uitgangspositie om gegevensbescherming verder te ontwikkelen. Tegelijkertijd ontbreekt een expliciete ontwikkelrichting. De hervormingsagenda biedt daarvoor weliswaar aanknopingspunten, maar is beperkt in reikwijdte.

Aanbeveling:

1. Onderzoek hoe het beleidsinstrumentarium kan worden bijgesteld om op een gestructureerde wijze ambities te formuleren, te sturen aan de hand van heldere KPI's, en het lerend vermogen van de organisatie te versterken. Overweeg daarbij een volwassenheidsmodel te hanteren.

Begripsgebruik en beleidsconsistentie

Binnen de organisatie worden termen als 'privacy', 'gegevensbescherming' en 'managementsysteem' niet altijd conform juridische of gangbare definities gebruikt. Dit leidt tot verwarring in beleid en uitvoering, en belemmert een eenduidige aanpak.

Aanbeveling:

2. Harmoniseer het begrippenkader en sluit aan bij de juridische terminologie uit de AVG en UAVG.

Governance en samenwerking

De rollen bij gegevensbescherming zijn helder belegd. In theorie is daarmee een solide basis gelegd. In de praktijk blijkt echter dat het samenspel binnen de eerste lijn en tussen de eerste, tweede en derde lijn niet altijd goed functioneert. Dit leidt tot een onevenwichtige belasting en knelpunten in de kwaliteit van DPIA's en andere processen.

Aanbevelingen:

3. Verduidelijk verantwoordelijkheden binnen en tussen organisatieonderdelen.
4. Stimuleer samenwerking tussen disciplines, maar streef daarbij wel naar rolvastheid.
5. Zorg voor een cultuur waarin iedereen aangesproken wordt op zijn rol en verantwoordelijkheden.
6. Zorg voorafgaand aan het inzetten van een generieke ICT-voorzieningen door een organisatieonderdeel voor beter inzicht bij het organisatieonderdeel in de risico's en maatregelen die voor die voorziening bekend zijn én voor voldoende afstemming om ervoor te zorgen dat bij het beoogde gebruik passende waarborgen zijn geïmplementeerd.

Beleid en standaarden

Het gegevensbeschermingsbeleid is gelaagd en breed opgezet, maar kent inconsistenties. Ook zijn standaarden niet altijd juridisch houdbaar of praktisch toepasbaar. Intussen wordt wel gewerkt aan een nieuw strategisch beleidskader voor alle IPM-domeinen samen.

Aanbevelingen:

7. Breng samenhang en onderlinge relaties tussen beleidsdocumenten expliciet in kaart en neem strijdigheden weg.
8. Zorg voor juridische consistentie en praktische toepasbaarheid.
9. Versterk en operationaliseer standaarden.

Risicobeheersing

De gemeente past diverse analysemethoden toe, waaronder DPIA's, BIO-gapanalyses en BIA's. De kwaliteit van DPIA's varieert op dit moment nog sterk. In 2025 maakt de gemeente een inhaalslag wat betreft het uitvoeren van BIO-gapanalyses. Op dit moment is daardoor nog niet altijd inzichtelijk of verwerkingen en systemen waarvoor de individuele organisatieonderdelen verantwoordelijk zijn aan de basisbeveiligingsmaatregelen voldoen.

Aanbevelingen:

10. Herzie het DPIA-format en proces, en sluit aan bij beproefde externe werkwijzen en richtsnoeren.
11. Stel in samenwerking met de FG toetsingscriteria op voor het aanbieden van DPIA's aan de FG, zodat voorafgaand daaraan in de eerste lijn al een kwaliteitstoets kan worden uitgevoerd.

ICT-ondersteuning

Voor kritieke processen binnen gegevensbescherming, zoals het verwerkingsregister en risicomanagement, wordt nog gewerkt met Excel. Dit is niet schaalbaar en vergroot de kwetsbaarheid van het beheer.

Aanbeveling:

12. Investeer in passende ICT-voorzieningen die het managementsysteem ondersteunen en sturing en toezicht faciliteren.

Privacy Enhancing Technologies (PET's)

Hoewel PET's zoals edge computing bij enkele verwerkingen succesvol zijn toegepast, blijkt dat aandacht voor de inzet van PET's bij DPIA-plichtige verwerkingen nog geen gemeengoed is.

Aanbeveling:

13. Onderzoek samen met partners hoe de inzet van PET's verbreed kan worden, en investeer in kennisontwikkeling op dit vlak.
14. Voer bij het toepassen van privacy-by-design standaard een analyse uit op de toepasbaarheid van PET's.

Bewustwording en training

Deelname aan de eLearning gegevensbescherming neem toe, maar blijft bij een aantal organisatieonderdelen achter. Dit geldt ook voor organisatieonderdelen waar zeer gevoelige gegevens over kwetsbare burgers worden verwerkt.

Van trainingen is niet altijd duidelijk hoe deze aansluiten op de rollen, taken en verantwoordelijkheden van de medewerkers die ze volgen.

Aanbevelingen:

15. Stuur nadrukkelijker op naleving van het bewustwordingsbeleid.
16. Investeer planmatig in kennisontwikkeling, afgestemd op rollen, taken en verantwoordelijkheden.

Toezicht door de FG

De FG ziet toe op inzet van AI en algoritmen, informatiebeveiliging, ethiek en samenwerking waarbij de bescherming van persoonsgegevens een rol speelt. De organisatie is zich niet altijd bewust van de reikwijdte van dit toezicht, wat leidt tot late betrokkenheid van de FG bij relevante initiatieven.

Aanbevelingen:

17. Betrek de FG vroegtijdig bij initiatieven waarbij de bescherming van persoonsgegevens een rol speelt, in het bijzonder bij technologische innovatie, ethische afwegingen en samenwerking met externe partijen.

Inleiding

Binnen de gemeentelijke organisatie is er veel aandacht voor gegevensbescherming. De inspanning die daarmee gepaard gaat, is aanzienlijk. Dat is logisch: de gemeente Utrecht is een grote organisatie met uiteenlopende wettelijke taken en bevoegdheden en grote (bestuurlijke) ambities op diverse terreinen. Deze taken en ambities gaan vaak gepaard met verwerkingen van persoonsgegevens, waarbij regelmatig sprake is van gevoelige gegevens over kwetsbare doelgroepen. De gemeente moet daarbij aantoonbaar voldoen aan de geldende gegevensbeschermingswet- en regelgeving. Dit vraagt om passend beleid en een zorgvuldige uitvoering gericht op het voldoen aan wettelijke vereisten en het voorkomen van risico's voor de rechten en vrijheden van burgers[1] of het terugbrengen daarvan tot een acceptabel niveau.

De FG houdt toezicht op de naleving van deze wet- en regelgeving en het beleid dat de organisatie daartoe voert. Tot en met 2021 bracht de FG jaarlijks verslag uit aan de drie bestuursorganen van de gemeente. In 2022 en 2023 werd, door persoonlijke omstandigheden, geen afzonderlijk jaarverslag opgesteld. Medio 2024 is alsnog een integraal verslag over beide jaren tot stand gekomen. Dit verslag is aangeboden aan de directie, maar door omstandigheden niet aan de verantwoordelijke bestuursorganen.

Over 2024 is geen jaarverslag opgesteld. In het laatste kwartaal van dat jaar nam de toenmalige FG – vanwege pensionering – afscheid van de gemeente. Sindsdien ben ik als nieuwe FG aangesteld. In overleg met de concerndirectie is besloten om een kort verslag op te stellen met mijn eerste waarnemingen, waarbij ik enkele bevindingen en aanbevelingen uit het verslag over 2022 en 2023 in ogenschouw neem. Waarnemingen zijn gebaseerd op advisering ten aanzien van tientallen uitgevoerde DPIA's en andere adviesgesprekken gevoerd met organisatieonderdelen – waaronder naar aanleiding van incidenten - in de periode januari tot en met juni 2025. Voor de totstandkoming van dit verslag zijn geen specifieke aanvullende onderzoeken uitgevoerd.

Ter volledigheid is het verslag van de vorige FG over 2022 en 2023 als bijlage opgenomen.

[1] Waar in dit verslag het begrip burgers wordt gebruikt, worden ook medewerkers bedoeld, als de gemeente daar gegevens over verwerkt.

Waarnemingen en aanbevelingen

Sturing

De gemeente Utrecht heeft de afgelopen jaren geïnvesteerd in een uitgebreid beleidsinstrumentarium voor gegevensbescherming en een passende gegevensbeschermingsorganisatie. Daardoor bevindt de gemeente zich in een goede positie om haar doelen op het gebied van gegevensbescherming te herijken en te sturen op de realisatie van deze doelen.

Het huidige beleidsinstrumentarium biedt hiervoor echter nog onvoldoende richting. De belangrijkste aanwijzing voor de toekomstige ontwikkeling van gegevensbescherming is te vinden in de hervormingsagenda, waarin de focus ligt op de kritieke processen. Voor gerichte sturing op ontwikkeling zijn aanvullende instrumenten nodig.

Een veelgebruikt instrument daarvoor is het hanteren van een volwassenheidsmodel. Met behulp van zo'n model kan de gemeente op gestructureerde wijze ambities formuleren, KPI's ontwikkelen voor monitoring en sturing, en het lerend vermogen van de organisatie versterken.

Ene dergelijk model kan de organisatie helpen ontwikkelen naar een – op het gebied van gegevensbescherming - meer anticiperende organisatie, die grip heeft op haar bedrijfsvoering, risico's tijdig signaleert en onderbouwd afweegt, en ontwikkelingen strategisch weet te benutten.

Aanbeveling

- Onderzoek hoe het beleidsinstrumentarium kan worden bijgesteld om op een gestructureerde wijze ambities te formuleren, te sturen aan de hand van heldere KPI's, en het lerend vermogen van de organisatie te versterken. Overweeg daarbij een volwassenheidsmodel te hanteren.

Heldere terminologie

Binnen de gemeente Utrecht gebruiken we termen als privacy, gegevensbescherming en managementsysteem op een manier die afwijkt van de juridische definities in wet- en regelgeving. Dit heeft gevolgen voor beleid, risicobeoordeling en communicatie.

Gegevensbescherming is een juridisch begrip uit de AVG en UAVG, gericht op het beschermen van persoonsgegevens. Privacy gebruiken we beleidsmatig als synoniem, hoewel dit woord niet voorkomt in de wet. Het verwijst vaak naar risico's voor de persoonlijke levenssfeer, terwijl de wet spreekt over risico's voor rechten en vrijheden van burgers. Vervolgens gebruiken we het begrip gegevensbescherming voor Informatiebeveiliging én juridische gegevensbescherming. Maar informatiebeveiliging richt zich op risico's voor de organisatie bij de verwerking van álle soorten gegevens, terwijl juridische gegevensbescherming draait om risico's voor betrokkenen bij de verwerking van persoonsgegevens.

Daarnaast gebruiken we het begrip gegevensbeschermingsmanagementsysteem (GBMS) voor een systeem dat zich op dit moment nog vooral op de beheersing van risico's richt. In de literatuur is een managementsysteem echter breder: het omvat het volledige stelsel van beleid, procedures en maatregelen om aan wetgeving te voldoen én risico's voor burgers te beheersen.

Aanbevelingen

18. Hanteer eenduidige definities in beleid en communicatie.
19. Gebruik het begrip gegevensbescherming in haar juridische betekenis.
20. Ontwikkel het GBMS door tot een breder managementsysteem dat voorziet in het totaal aan maatregelen en beleid dat nodig is om persoonsgegevens rechtmatig, behoorlijk en transparant te verwerken.

Governance en samenwerking

Binnen de gemeente is zowel in beleid als in uitvoering een robuuste gegevensbeschermingsorganisatie ingericht. Rollen, taken en verantwoordelijkheden zijn belegd met als doel gegevensbescherming structureel te borgen in de organisatie.

Er zijn adviseurs aangesteld die verantwoordelijk zijn voor het vormgeven, evalueren, bijstellen, toepassen en bewaken van het organisatiebrede managementsysteem, inclusief de bijbehorende standaarden en procedures. Daarnaast ondersteunen en adviseren DISO's de organisatieonderdelen bij de uitvoering. Ook auditors besteden een deel van hun inspanningen aan het toetsen van gegevensbescherming binnen de organisatie.

In theorie is hiermee een solide basis gelegd om gegevensbescherming in alle lijnen van de organisatie te verankeren. In de praktijk doen zich echter structurele knelpunten voor**.**

Samenspel van disciplines in de eerste en tweede lijn

Binnen een publieke organisatie is het samenspel tussen verschillende disciplines essentieel voor een zorgvuldige en rechtmatige gegevensverwerking. Een goede samenwerking tussen proceseigenaren, juridisch adviseurs, informatieadviseurs, recordmanagers, (functioneel) beheerders en DISO's draagt bij aan een effectieve risicoanalyse en borging van gegevensbescherming.

Kennis van de relevante (juridische) kaders en bestuurlijke doelen is daarbij cruciaal. Dit vraagt om inzicht in de wettelijke taak of bevoegdheid, de bestuurlijke doelen die daarbij zijn bepaald, de inrichting van het uitvoeringsproces en eventuele (contractuele) afspraken met externe partijen.

In de praktijk blijkt dat het ontbreken van deze samenwerking kan leiden tot onvolledige beschrijvingen van verwerkingen, onduidelijke juridische grondslagen, waarbij doelen niet aansluiten bij het juridisch kader, de uitvoering niet aansluit bij contractuele afspraken of maatregelen die niet worden opgepakt. Ook belemmert het de ruimte voor de DISO om beleid op het niveau van een organisatieonderdeel uit te werken.

Het versterken van deze samenwerking draagt bij aan een beter begrip van verantwoordelijkheden en een meer geïntegreerde aanpak van gegevensbescherming.

Samenspel tussen organisatieonderdelen in de eerste lijn

Bij de inrichting van generieke ICT-voorzieningen lijkt er ruimte voor verbetering in de afstemming tussen organisatieonderdelen. Voorzieningen voldoen daardoor niet altijd aan de vereisten op het gebied van gegevensbescherming die voor de ondersteunde processen vereist is.

We zien op dit moment dat met name het beveiligen van persoonsgegevens, samenspel vraagt tussen verschillende organisatieonderdelen. Dit samenspel verloopt niet altijd naar behoren. Zo heeft niet elk organisatieonderdeel voldoende inzicht in de risico's en maatregelen die voor generieke ICT-voorzieningen bekend zijn. Ook gebruiken organisatieonderdelen systemen soms op manieren die bij de systeemeigenaar niet bekend zijn. Daardoor kunnen onverwachte risico's optreden. Enkele voorbeelden daarvan beschrijf ik in bijlage 1 van dit verslag.

Samenspel tussen de drie lijnen

Wanneer het samenspel in de eerste lijn onvoldoende is, komt de uitvoering van gegevensbescherming disproportioneel bij de DISO terecht, Dit maakt het voor de DISO lastig om in zijn rol te blijven. Met name diens rol bij het borgen van de kwaliteit leidt daar onder. Als de tweede en derde lijn hun rol wel vasthouden, kan dit leiden tot onvrede in de uitvoering. Doen ze dat niet, dan vervaagt de rolverdeling tussen lijnen, waardoor het kwaliteitssysteem onder druk komt te staan.

In de context van bijvoorbeeld de DPIA betekent dit dat de DISO onvoldoende in staat is om een kwaliteitstoets uit te voeren voordat deze risicoanalyses aan de FG in de derde lijn worden voorgelegd. Hierdoor wordt de inzet van de FG bij de toetsing en advisering onevenredig groot: via adviesnotities probeert de FG bij te sturen op de kwaliteit..

Aanbevelingen

- Werk het gegevensbeschermingsbeleid verder uit zodat helder wordt wie binnen een organisatieonderdeel concreet welke bijdrage moet verzorgen, zodat gegevensbescherming adequaat kan worden vormgegeven.
- Zorg voor een cultuur waarin iedereen aangesproken wordt op zijn rol en verantwoordelijkheden..
- Onderzoek of de huidige inrichting van generieke voorzieningen en of de technische en organisatorische beschermingsmaatregelen daaromheen, geschikt zijn voor het feitelijke gebruik en voer waar mogelijk verbeteringen door.
- Zorg voorafgaand aan het inzetten van een generieke ICT-voorzieningen door een organisatieonderdeel voor beter inzicht bij het organisatieonderdeel in de risico's en maatregelen

die voor die voorziening bekend zijn én voor voldoende afstemming om ervoor te zorgen dat bij het beoogde gebruik passende waarborgen zijn geïmplementeerd.

Beleid en standaarden

De gemeente beschikt over een uitgebreid en gelaagd gegevensbeschermingsbeleid. Dit begint bij de gemeentelijke privacyverordening en wordt via het strategisch beleid en het Gegevensbeschermingsmanagementsysteem (GBMS) verder uitgewerkt in strategische en tactische standaarden, processen en formats. Deze gelaagdheid draagt bij aan overzichtelijkheid en hanteerbaarheid, en biedt medewerkers steeds meer concrete handvatten om invulling te geven aan hun verantwoordelijkheden op het gebied van gegevensbescherming. Intussen wordt overigens wel gewerkt aan een nieuw strategisch beleidskader voor alle IPM-domeinen samen.

Het is van belang dat voor alle betrokkenen duidelijk is hoe de verschillende beleidsdocumenten zich tot elkaar verhouden, en dat deze documenten inhoudelijk op elkaar zijn afgestemd. Hier wringt het in de praktijk. Zo is er sprake van inconsistentie tussen de privacyverordening, toezeggingen van het college aan de raad, en het uitvoeringsbeleid. Waar bijvoorbeeld de privacyverordening voorschrijft dat de (FG) datalekken meldt bij de Autoriteit Persoonsgegevens, is deze taak inmiddels belegd bij de organisatieonderdelen. Het bijhouden van het register van verwerkingen is gedecentraliseerd. Daarnaast is een openbaar register van datalekken niet langer beschikbaar, ondanks een toezegging daarover van college aan de raad.

Ook van andere beleidsinstrumenten is niet altijd duidelijk hoe deze elkaar beïnvloeden. Zo schrijft het GBMS voor dat risico's zowel bruto (vóór het nemen van maatregelen) als netto (na het nemen van maatregelen) worden gewaardeerd. Daar wordt echter niet altijd naar verwezen in de kaders voor de uitvoering van verschillende soorten risicoanalyses die binnen de gemeente worden toegepast. Dit leidt tot uiteenlopende interpretaties en werkwijzen onder medewerkers.

Aanbevelingen

- Evalueer het samenspel tussen beleidsdocumenten. Breng de onderlinge samenhang in kaart en stel documenten waar nodig bij of trek ze in. Dit voorkomt tegenstrijdigheden en bevordert consistentie in beleid en uitvoering.
- Zorg voor juridische consistentie. Breng standaarden waar nodig beter in lijn met geldende wettelijke vereisten, zodat de juridische houdbaarheid van het beleid gewaarborgd blijft.
- Versterk en operationaliseer standaarden. Werk een aantal bestaande standaarden verder uit, zodat deze meer richting geven aan de uitvoeringsorganisatie. Toets de toepasbaarheid ervan doorlopend in de praktijk. Dit vergemakkelijkt de implementatie in de eerste lijn, bevordert uniforme toepassing en maakt de uitvoering van gegevensbescherming beter uitlegbaar. Het uiteindelijke doel is dat medewerkers – op elk niveau – beschikken over duidelijk handelingsperspectief bij de bescherming van persoonsgegevens.

Risicobeheersing

De beheersing van risico's is beleidsmatig geborgd in het GBMS. De gemeente Utrecht past ter uitvoering daarvan een toenemend aantal en soorten risico- en impactanalyses (zoals de BIO-gapanalyse, DPIA's, BIA's, ORA's, TRA's, PRA's) toe en stelt deze - bij wijzigingen in systemen of processen - bij. Ze neemt naar aanleiding daarvan maatregelen om risico's voor burgers én de organisatie te beperken en onrechtmatige, onbehoorlijke of niet-transparante gegevensverwerking te voorkomen. De hierboven vermelde analyses vormen ook bronnen voor de uitvoering van een DPIA. Ze worden bijvoorbeeld gebruikt voor het op operationeel en tactisch niveau in kaart brengen van de mate waarin standaard beveiligingsmaatregelen zijn genomen en van resterende risico's voor de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en daarmee samenhangend de bedrijfscontinuïteit.

In de periodieke inventarisatie door de CIO – de Monitor Gegevensbescherming – is de stand van zaken ten aanzien van de uitvoering van alle bovenstaande analysemethoden opgenomen, behalve die voor de BIO-gapanalyse. Deze werden op de organisatieonderdelen namelijk nog niet uitgevoerd. In 2025 maakt de gemeente een inhaalslag. Op dit moment is daardoor nog niet altijd inzichtelijk of verwerkingen en systemen waarvoor de individuele organisatieonderdelen verantwoordelijk zijn, aan de basisbeveiligingsmaatregelen voldoen.

Standaard voor DPIA's

DPIA's worden ter advies aan de FG voorgelegd. Waar we spreken over een DPIA, bedoelen we overigens vaak het DPIA-verslag. Het uitvoeren van een DPIA is namelijk een proces. Het verslag is een weergave van de uitvoering en de uitkomsten van dat proces.

In de verslagperiode legde de organisatie tientallen DPIA's aan mij voor. Een DPIA wordt uitgevoerd om risico's voor de rechten en vrijheden van betrokkenen in beeld te brengen en om passende maatregelen te definiëren ter beperking van die risico's. Om dit doel te bereiken moeten DPIA's een redelijke mate van diepgang hebben. Denk hierbij aan inzicht in:

- Het juridische kader van de gegevensverwerking.
- Het feitelijke verwerkingsproces.
- Het samenspel tussen doelen, gegevens, partijen en systemen binnen de stappen van het verwerkingsproces.

Deze elementen zijn essentieel om risico's op basis van inhoudelijk inzicht te kunnen identificeren en beoordelen.

De gemeente kent een standaard proces en format voor de uitvoering en verslaglegging van DPIA's. Al meer dan een jaar wordt aan de evaluatie en herijking daarvan gewerkt. Dit is opvallend, aangezien er buiten de organisatie verschillende beproefde handreikingen, formats en richtsnoeren beschikbaar zijn die zich sinds de invoering van de AVG bewezen hebben. De status van de evaluatie en herijking is op dit moment onduidelijk. Daarom richt ik me in het onderstaande op het geldend beleid.

Hoewel een DPIA (deels) openbaar gemaakt mag worden zodat deze voor betrokkenen inzichtelijk is, mag het werkelijke doel van het uitvoeren van een DPIA daarbij niet uit het oog verloren worden. Volgens het huidige beleid worden DPIA's echter opgesteld voor betrokkenen, oftewel de personen van wie gegevens worden verwerkt. Dit onjuiste uitgangspunt heeft grote impact op de wijze waarop DPIA's worden gedocumenteerd. In het huidige format is er ook nog weinig aandacht voor de aantoonbaarheid van het gevolgde DPIA-proces; het verslag richt zich uitsluitend op de uitkomsten.

Vanzelfsprekend mag een DPIA voortbouwen op bestaande procesdocumentatie en analyses, bijvoorbeeld op het gebied van informatiebeveiliging. Dat is mogelijk wanneer deze producten voldoende aansluiten bij de doelstellingen van een DPIA. Momenteel worden dergelijke analyses echter niet standaard aan de DPIA's toegevoegd. Dat is een gemiste kans, want daardoor geven DPIA's geen volledig beeld van de geïdentificeerde risico's en maatregelen die bij het proces in kaart zijn gebracht.

Door de bovenstaande knelpunten draagt het huidige beleidskader niet altijd bij aan DPIA's van voldoende kwaliteit. Ook worden werkwijzen niet consequent toegepast. Dit geldt bijvoorbeeld bij het tot stand komen van DPIA's voor het toepassen van de risicowaardering volgens het GBMS.

Daarnaast speelt ook het al genoemde samenspel van disciplines in de eerste lijn en de druk op de werking van het 'three lines model', een belangrijke rol. De kwaliteit van DPIA's die de afgelopen maanden aan mij zijn voorgelegd, varieert dan ook sterk.

Aanbevelingen

- Maak gebruik van beschikbare werkwijzen en richtsnoeren van buiten de organisatie om het eigen DPIA-proces en -verslag te verbeteren, denk bijvoorbeeld aan de documenten van de Rijksoverheid.
- Voeg alle bestaande analyses en procesdocumentatie aan DPIA's toe.
- Breidt waar mogelijk bestaande instrumenten - zoals procestekeningen - uit zodat deze ook bruikbaar zijn in de context van gegevensbescherming.
- Herzie de standaard voor DPIA's, zodat aantoonbaarheid van het gevolgde proces en de betrokken disciplines beter wordt geborgd, een passende inhoudelijke uitvoering wordt gefaciliteerd, en helder is welke bijdrage van elke betrokken discipline wordt verwacht.
- Stel in samenwerking met de FG toetsingscriteria op voor het aanbieden van DPIA's aan de FG, zodat voorafgaand daaraan in de eerste lijn al een kwaliteitstoets kan worden uitgevoerd.

Ondersteunende voorzieningen en bevorderende technieken

Ondersteunende voorzieningen

Opvallend is dat een grote organisatie als de gemeente, met honderden verwerkingen en tientallen medewerkers die bijdragen aan bijvoorbeeld het verwerkingsregister, hiervoor primair gebruikmaakt van Microsoft Excel. Deze keuze brengt beperkingen met zich mee in termen van schaalbaarheid, betrouwbaarheid en beheer, en vergroot de kwetsbaarheid van het register als beheersinstrument.

Ditzelfde zien we terug bij risicomanagement. Daarvoor zijn op dit moment buiten Domstad IT geen passende ICT-voorzieningen ingericht. Een actueel totaaloverzicht van de status van risicoanalyses, risico's, voorgenomen maatregelen en eigenaarschap, is daardoor niet voorhanden. Slecht één maal per 4 maanden is er beperkt inzicht met behulp van zelfrapportage middels Excel door de individuele organisatieonderdelen.

Dergelijke beperkte ondersteuning door ICT-voorzieningen zorgt voor een onnodig hoge belasting van de gegevensbeschermingsorganisatie en onvoldoende actueel inzicht in de staat van gegevensbescherming in de organisatie.

Aanbeveling

- Richt bewezen en functionele ICT-voorzieningen in om het volledige gegevensbeschermingsmanagementsysteem (GBMS) te kunnen beheersen, aantoonbaar te maken en effectief te ondersteunen bij sturing en toezicht.

Gegevensbescherming-bevorderende technieken (privacy enhancing technologies, PET's)

De gemeente past in steeds meer situaties data-gedreven en data-gestuurd werken toe. De ontwikkeling en inzet van gegevensbescherming-bevorderende technieken (PET's) kan in die omstandigheden bijdragen aan de bescherming van persoonsgegevens, vooral in situaties waarin persoonsgegevens van meerdere verwerkingen bij elkaar gebracht worden voor bijvoorbeeld analyses voor wetenschappelijke of statistische doeleinden, historisch onderzoek of beleidsontwikkeling.

Maar ook in andere situaties kunnen PET's bijdragen aan de bescherming van persoonsgegevens omdat ze bijdragen aan privacy-by-design. Een mooi voorbeeld van succesvolle inzet van PET's bij gemeentelijke verwerkingen, is de inzet van edge computing in sensoren voor het analyseren van verkeersstromen en het detecteren van gevaarlijke verkeerssituaties. Daarbij worden camerabeelden al in de sensoren omgezet in abstracte informatie over bewegingen van soorten voertuigen die niet meer herleidbaar zijn naar personen. De doelen van de gemeente worden zo nagestreefd met minimale verwerking van persoonsgegevens. Dit levert voordelen op voor burgers én de gemeente: de persoonlijke levenssfeer wordt beschermd (mobiliteitspatronen van individuele burgers worden niet gevolgd) en op de investeringen in de beveiliging van de verzamelde informatie kan aanzienlijk worden bespaard. Toch blijkt dat aandacht voor de inzet van PET's bij DPIA-plichtige verwerkingen nog geen gemeengoed is.

Aanbevelingen

- Onderzoek samen met partners hoe de inzet van PET's verbreed kan worden, en investeer in kennisontwikkeling op dit vlak.
- Voer bij het toepassen van privacy-by-design standaard een analyse uit op de toepasbaarheid van PET's.

Bewustwording en training

Uit de periodieke inventarisatie door het CIO Office – de Monitor Gegevensbescherming - blijkt dat er een grote toename is in het aantal medewerkers dat deelneemt aan de eLearning gegevensbescherming, maar ook dat er nog een significant aantal organisatieonderdelen is waar een aanzienlijk deel van de medewerkers de eLearning nog niet tot het afgesproken niveau hebben doorlopen. Dit geldt ook voor organisatieonderdelen waar zeer gevoelige gegevens over kwetsbare burgers worden verwerkt.

Soms is niet duidelijk in hoeverre trainingen voor medewerkers zijn afgestemd op hun rollen, taken en verantwoordelijkheden. Bijvoorbeeld op het gebied van AI.

Aanbevelingen

- Stuur nadrukkelijker op de naleving van het bewustwordingsbeleid.
- Investeer planmatig in kennisontwikkeling die aansluit op de rollen, taken en verantwoordelijkheden van medewerkers.

Toezicht door de FG

De FG ziet toe op de naleving van wet- en regelgeving rondom gegevensbescherming, zoals de AVG, UAVG, Wpg en relevante gemeentelijke kaders. Deze wetgeving richt zich op de verwerking van persoonsgegevens en de bescherming van de rechten en vrijheden van burgers, zoals vastgelegd in het EU-Grondrechtenhandvest. Goed toezicht door de FG draagt bij aan rechtmatige, zorgvuldige en transparante gemeentelijke dienstverlening.

Het toezicht van de FG strekt zich uit over meerdere domeinen binnen de organisatie. Daar is de organisatie zich niet altijd (tijdig) bewust van, terwijl het juist van belang is om de FG tijdig te betrekken. Enkele voorbeelden:

- **AI en nieuwe technologieën**

  Zodra technologieën zoals AI of RPA van invloed zijn op de verwerking van persoonsgegevens, vallen ze onder het toezicht van de FG.

- **Informatiebeveiliging**

  De wetgever verlangt dat de gemeente passende technische en organisatorische maatregelen neemt om een op het risico afgestemd beveiligingsniveau te waarborgen bij het verwerken van persoonsgegevens. De FG ziet daar op toe.

- **Ethiek**

  Ethiek speelt een rol wanneer verwerking van persoonsgegevens mogelijk leidt tot een onevenredige inbreuk op rechten en vrijheden. Uthiek-assessments vallen dan binnen het toezicht van de FG.

- **Samenwerkingsverbanden**

  Bij samenwerking met andere partijen is de FG verantwoordelijk voor toezicht op verwerkingen binnen de gemeentelijke verantwoordelijkheid. Bij gezamenlijke verantwoordelijkheid, zoals bij het RIEC en het Zorg- en Veiligheidshuis, is samenwerking tussen FG's vereist. De FG van Utrecht is wettelijk aangewezen als coördinerend FG voor de genoemde samenwerkingsverbanden.

Aanbevelingen

- Betrek de FG vroegtijdig bij initiatieven waarbij de bescherming van persoonsgegevens een rol speelt, in het bijzonder bij technologische innovatie, ethische afwegingen en samenwerking met externe partijen.

Bijlage 1: Voorbeelden generieke ICT-voorzieningen

Het zaaksysteem

Het zaaksysteem kent enkele aandachtspunten bij de verwerkingen van BRP-gegevens. Zo zoekt het systeem automatisch in de landelijke voorziening waarin ook BRP gegevens zitten van burgers die niet in de gemeente Utrecht wonen. Dergelijke gegevens mag de gemeente echter slechts voor een beperkt aantal taken gebruiken.

Daarnaast maken sommige organisatieonderdelen bijvoorbeeld gebruik van exportfuncties van deze BRP-gegevens om knelpunten door beperkingen in de eigen ICT-voorzieningen te verhelpen. Hoewel dergelijke 'workarounds' bij voorkeur worden vermeden, vragen ze in ieder geval om passend autorisatiebeheer en voorzieningen voor het registreren en controleren van het (rechtmatig) gebruik van persoonsgegevens (logging en monitoring). Dit vraagt om voldoende afstemming door de organisatieonderdelen met de systeemeigenaar voorafgaand aan het inzetten van een systeem om ervoor te zorgen dat bij het beoogde gebruik passende waarborgen zijn geïmplementeerd.

Teams

Microsoft Teams wordt binnen de organisatie regelmatig ingezet voor verwerkingen waarvoor het inrichten van een eigen ICT-voorziening niet haalbaar is. Dat kunnen ook kleinere, maar gevoelige verwerkingen zijn, zoals bij data-analyse of multidisciplinaire casusregie. Dergelijke processen vragen om passend autorisatiebeheer en voorzieningen voor het registreren en controleren van het (rechtmatig) gebruik van persoonsgegevens (logging en monitoring). Op dit moment is er voorafgaand aan het inzetten van een systeem nog niet altijd voldoende afstemming door de organisatieonderdelen met de systeemeigenaar om ervoor te zorgen dat dergelijke waarborgen voor het beoogde gebruik op een passende wijze zijn geïmplementeerd.

Bijlage 2: Voorbeelden standaarden

Standaard voor het verwerkingsregister

De gemeente hanteert één gezamenlijk en zeer uitgebreid register van verwerkingsactiviteiten voor alle drie gemeentelijke bestuursorganen (de verwerkingsverantwoordelijken) en voor beide regimes: de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg). Hoewel dit register een belangrijke stap is richting transparantie en verantwoording, kent het enkele inhoudelijke en organisatorische tekortkomingen. Zo wordt in het register niet de formele verwerkingsverantwoordelijke vermeld, maar een intern contactpersoon. Hierdoor is voor betrokkenen niet zichtbaar welk bestuursorgaan verantwoordelijk is voor een specifieke verwerking. Ook wordt eventuele gezamenlijke verwerkingsverantwoordelijkheid niet inzichtelijk gemaakt. Daarnaast erkent de standaard uitsluitend externe ontvangers, terwijl ook interne verstrekkingen met een ander doel of grondslag juridisch als 'ontvanger' kwalificeren.

Standaarden voor de rechten van betrokkenen

In 2024 beschikte de gemeente over een standaardproces voor de afhandeling van inzageverzoeken. Deze standaard voldeed echter niet aan alle wettelijke vereisten. Zo ontbrak de verplichte verwijzing naar andere rechten van betrokkenen in het besluit op een inzageverzoek. Deze tekortkoming is in de eerste helft van 2025 geadresseerd in een vernieuwde standaard, die momenteel wordt geïmplementeerd.

Voor de overige rechten van betrokkenen (zoals rectificatie, verwijdering, beperking van verwerking, bezwaar en overdraagbaarheid) was geen standaardproces ingericht. De gemeente ging ervan uit dat betrokkenen zich rechtstreeks tot het betreffende organisatieonderdeel zouden wenden. Dit leidt in de praktijk tot knelpunten, bijvoorbeeld bij het vaststellen van de identiteit van de verzoeker en bij het correct adresseren van het verzoek binnen de organisatie.

Standaard voor transparantie

De gemeente geeft invulling aan haar transparantieverplichtingen (artikelen 12-14 AVG en 24a-24b Wpg) via een gelaagde aanpak. Enerzijds door middel van algemene privacyverklaringen per domein (zoals onderzoek, cameratoezicht, vergunningverlening en zorg), anderzijds via het openbaar gepubliceerde verwerkingsregister. Zoals hierboven beschreven, kent dit register echter beperkingen.

Elk organisatieonderdeel is verantwoordelijk voor het beoordelen of deze twee instrumenten voldoende zijn om aan de transparantieverplichtingen te voldoen, en voor het aanvullen van informatie richting burgers waar nodig. Uit verslagen van DPIA's blijkt echter dat organisatieonderdelen zich hier niet altijd voldoende van bewust zijn. In de praktijk wordt vaak volstaan met een verwijzing naar de algemene privacyverklaring en het verwerkingsregister, waardoor de transparantie richting betrokkenen tekortschiet. In sommige gevallen wordt transparantie in een DPIA helemaal niet geadresseerd, ervan uitgaand dat dit organisatiebreed is georganiseerd.